anand guru

SOC EXPERTS

Interview Questions on **Computer Networking**

Anand Guru

Security+ | CySA+ | CEH | ECIH

Founder

SOC Experts

https://socexperts.com

Network Device

What is a Hub?

Hub is a layer 1 device that connects multiple computers. Hub is usually terms as 'dumb' device because it broadcasts all the data to every port.

What is a Switch?

Switch is a layer 2 device that connect two or more computers.

Switch can decide which computer is the message intended for and send the message directly to the right computer (instead of a broadcast).

What is a Router?

Router is a layer 3 device that connect 2 or more networks.

Routers can calculate the best route for sending data from one point to another using routing protocols.

What are the ranges of Private IP?

Private IP addresses are also called as **Non-Routable IP Addresses.**

The ranges are

- Class A 10.0.0.0 – 10.255.255.255
- Class B 172.16.0.0 – 172.31.255.255
- Class C 192.168.0.0 – 192.168.255.255

CIDR format

- 10.0.0.0/8
- 172.16.0.0/12
- 192.168.0.0/16

What is NAT?

NAT Stands for **Network Address Translation**

It is the process of converting one IP to another. Usually a Private IP to a Public IP and vice versa.

What is PAT?

PAT stands for **Port Address Translation**

PAT permits multiple devices on a LAN to be mapped to a single public IP address. The goal of PAT is to conserve public IP addresses.

Example:

If traffic to 100.20.30.40 is coming on **Port 22** → NAT that to 10.10.5.6 (A Linux server)

If traffic to 100.20.30.40 is coming on **Port 443** → NAT that to 10.10.5.7 (Web server)

Commonly used Port Numbers

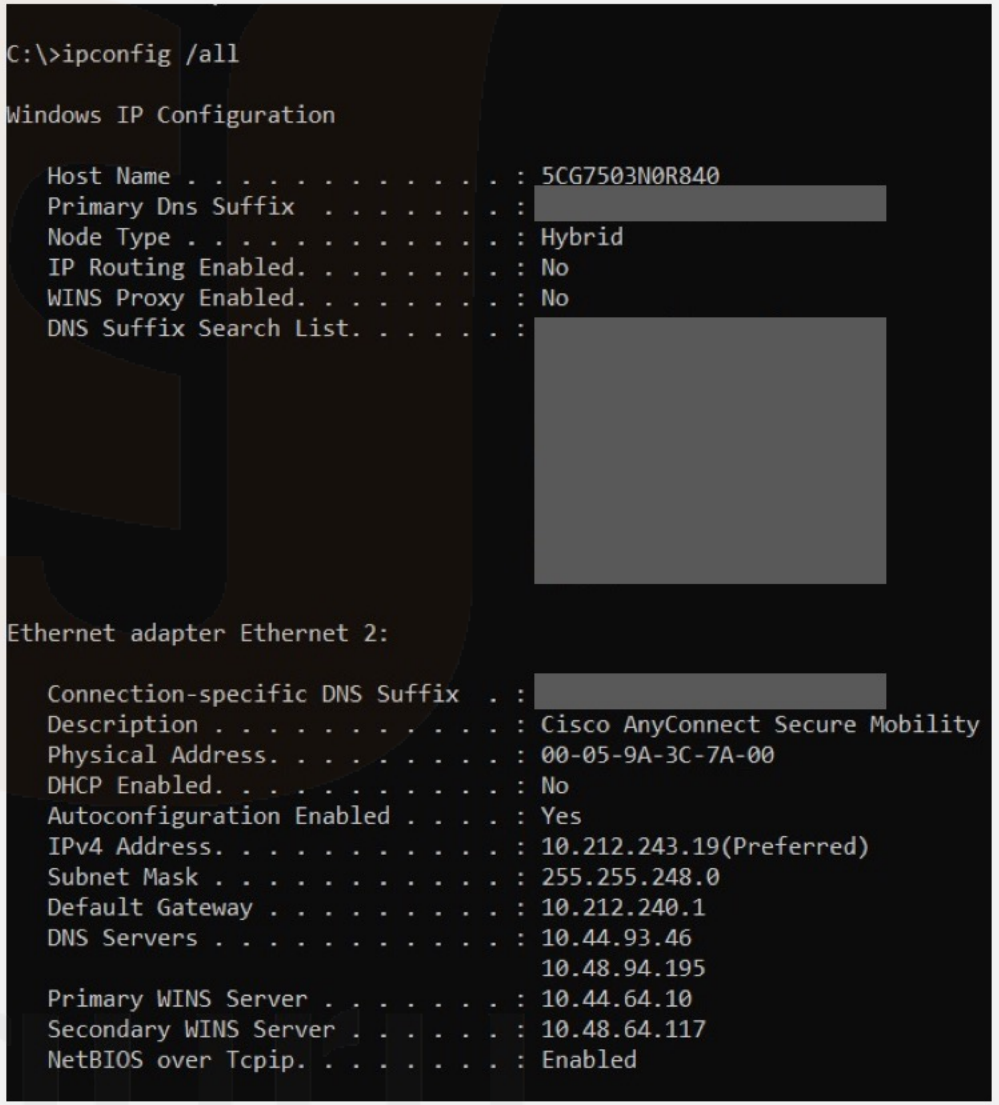
Protocol	Service	Port Number
FTP	File Transfer Protocol	20, 21
Telnet	Telnet	23
SSH	Secure Shell	22
SMTP	Simple Mail Transfer Protocol	25
DNS	Domain Name System	53
DHCP	Dynamic Host Configuration Protocol	67, 68
HTTP	Hyper Text Transfer Protocol	80
POP3	Post Office Protocol	110
NTP	Network Time Protocol	123
NetBIOS	NetBIOS Name Service	135 - 139
IMAP	Internet Message Access Protocol	143

Protocol	Service	Port Number
SNMP	Simple Network Management Protocol	161, 162
LDAP	Lightweight Directory Access Protocol	389
HTTPS	Secure Hyper Text Transfer Protocol	443
MS SQL	Microsoft SQL	1433
MySQL	mySQL Database	3306
RDP	Remote Desktop Protocol	3389
Syslog	Used to send logs to remote server	514
TLS Syslog	Secure Syslog	6514
SFTP	Secure File Transfer Protocol	22
Secure SMTP	Secure Simple Mail Transfer Protocol	587

anand guru

Networking Basic Command Line Tools.

- How to find the IP address of a machine?
  `ipconfig`
- How to find the MAC address of a machine?
  `ipconfig /all`
- What is MAC address listed as in Windows machine?
  Physical Address
- How do you find if DHCP is enabled on a system?
  `ipconfig /all`
- How do you find the Default Gateway on the system?
  `ipconfig /all`
- How do you find DNS servers on a system?
  `ipconfig /all`


C:\>ipconfig /all
Windows IP Configuration
Host Name . . . . . : 5CG7503N0R840
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No
DNS Suffix Search List. . . . . :
Ethernet adapter Ethernet 2:
Connection-specific DNS Suffix . :
Description . . . . . : Cisco AnyConnect Secure Mobility
Physical Address. . . . . : 00-05-9A-3C-7A-00
DHCP Enabled. . . . . : No
Autoconfiguration Enabled . . . . : Yes
IPv4 Address. . . . . : 10.212.243.19(Preferred)
Subnet Mask . . . . . : 255.255.248.0
Default Gateway . . . . . : 10.212.240.1
DNS Servers . . . . . : 10.44.93.46
10.48.94.195
Primary WINS Server . . . . . : 10.44.64.10
Secondary WINS Server . . . . . : 10.48.64.117
NetBIOS over Tcpip. . . . . : Enabled

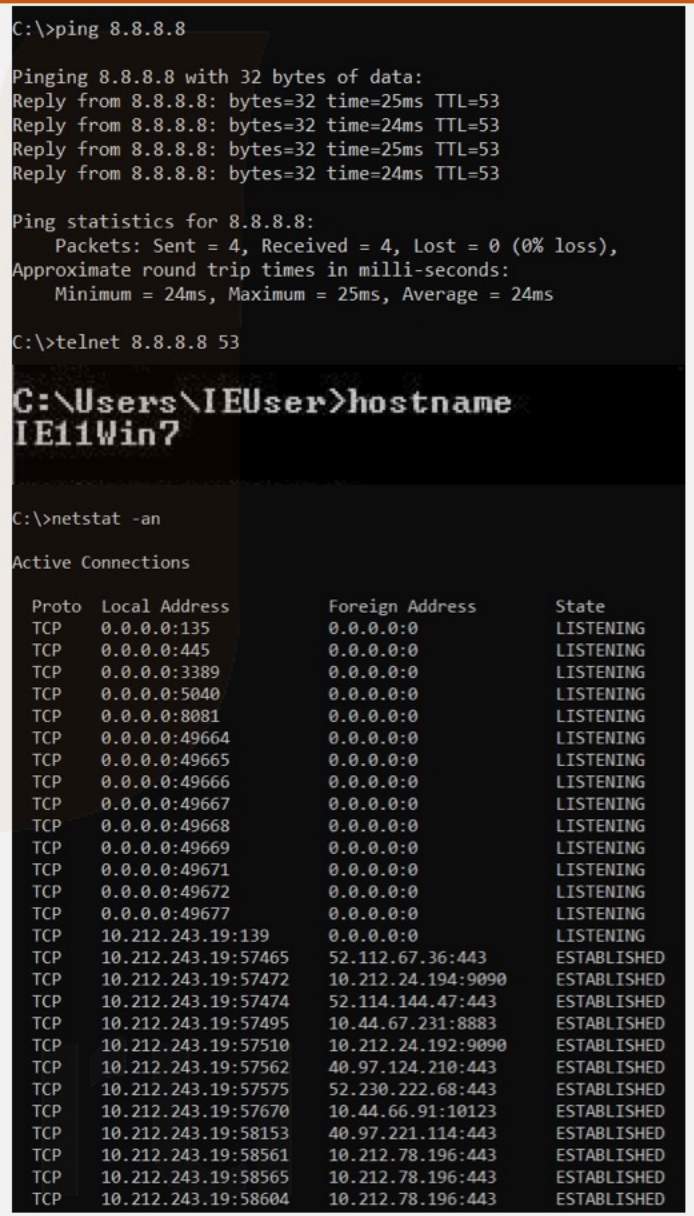
Networking Basic Command Line Tools.

- How do you check if the destination machine is up and running or reachable?
  `ping`

- How to check if a port is open on the destination server?
  `telnet`
  telnet is done on the port in question.

- How to get the hostname of a machine?
  `hostname`

- How do you check open port on a machine?
  `netstat -an`


C:\>ping 8.8.8.8
Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=25ms TTL=53
Reply from 8.8.8.8: bytes=32 time=24ms TTL=53
Reply from 8.8.8.8: bytes=32 time=25ms TTL=53
Reply from 8.8.8.8: bytes=32 time=24ms TTL=53
Ping statistics for 8.8.8.8:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 24ms, Maximum = 25ms, Average = 24ms
C:\>telnet 8.8.8.8 53
C:\Users\IEUser>hostname
IE11Win7
C:\>netstat -an
Active Connections
Proto Local Address Foreign Address State
TCP 0.0.0.0:135 0.0.0.0:0 LISTENING
TCP 0.0.0.0:445 0.0.0.0:0 LISTENING
TCP 0.0.0.0:3389 0.0.0.0:0 LISTENING
TCP 0.0.0.0:5040 0.0.0.0:0 LISTENING
TCP 0.0.0.0:8081 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49664 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49665 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49666 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49667 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49668 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49669 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49671 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49672 0.0.0.0:0 LISTENING
TCP 0.0.0.0:49677 0.0.0.0:0 LISTENING
TCP 10.212.243.19:139 0.0.0.0:0 LISTENING
TCP 10.212.243.19:57465 52.112.67.36:443 ESTABLISHED
TCP 10.212.243.19:57472 10.212.24.194:9090 ESTABLISHED
TCP 10.212.243.19:57474 52.114.144.47:443 ESTABLISHED
TCP 10.212.243.19:57495 10.44.67.231:8883 ESTABLISHED
TCP 10.212.243.19:57510 10.212.24.192:9090 ESTABLISHED
TCP 10.212.243.19:57562 40.97.124.210:443 ESTABLISHED
TCP 10.212.243.19:57575 52.230.222.68:443 ESTABLISHED
TCP 10.212.243.19:57670 10.44.66.91:10123 ESTABLISHED
TCP 10.212.243.19:58153 40.97.221.114:443 ESTABLISHED
TCP 10.212.243.19:58561 10.212.78.196:443 ESTABLISHED
TCP 10.212.243.19:58565 10.212.78.196:443 ESTABLISHED
TCP 10.212.243.19:58604 10.212.78.196:443 ESTABLISHED

Explain the difference Between TCP and UDP.

	TCP	UDP
✓	Transmission Control Protocol	User Datagram Protocol
✓	Connection Oriented	Connection Less
✓	Acknowledgement for each packet transmitted	No Acknowledgement
✓	Failed packets are retransmitted	No re-transmission
✓	Guaranteed delivery	Best effort delivery
✓	Reliable	Unreliable
✓	TCP is slower	UDP is faster
✓	Example: HTTP, HTTPS, SMTP, SSH etc.	Streaming Videos, VOIP Calls, Online Games etc.

anand guru

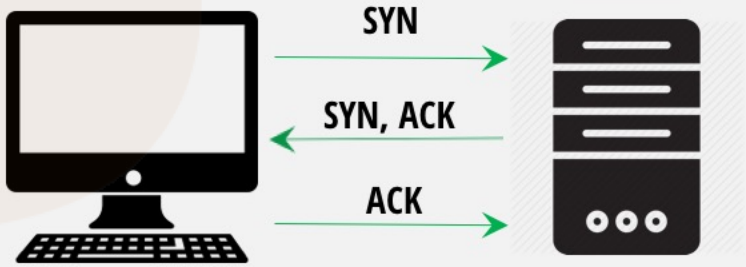
Explain 3 way handshake.

A three-way handshake is a method used in a TCP/IP network to create a connection between two hosts.

It is a 3 step process that requires both the client and server to exchange SYN and ACK (acknowledgment) packets before actual data communication begins.

Process is as Follows:

- A client node sends a **SYN** data packet to a server it wants to communicate to. The objective of this packet is to ask/infer if the server is open for new connections.
- If the server is willing to communicate to the client (if the port is open) it responds with an ACK packet.
  - It also expresses its intention of talking back to the client with its SYN packet.
  - Together it is **SYN/ACK**
- The client node responds with an **ACK** for the server's SYN.



Upon completion of this process, the connection is created and the host and server can communicate.

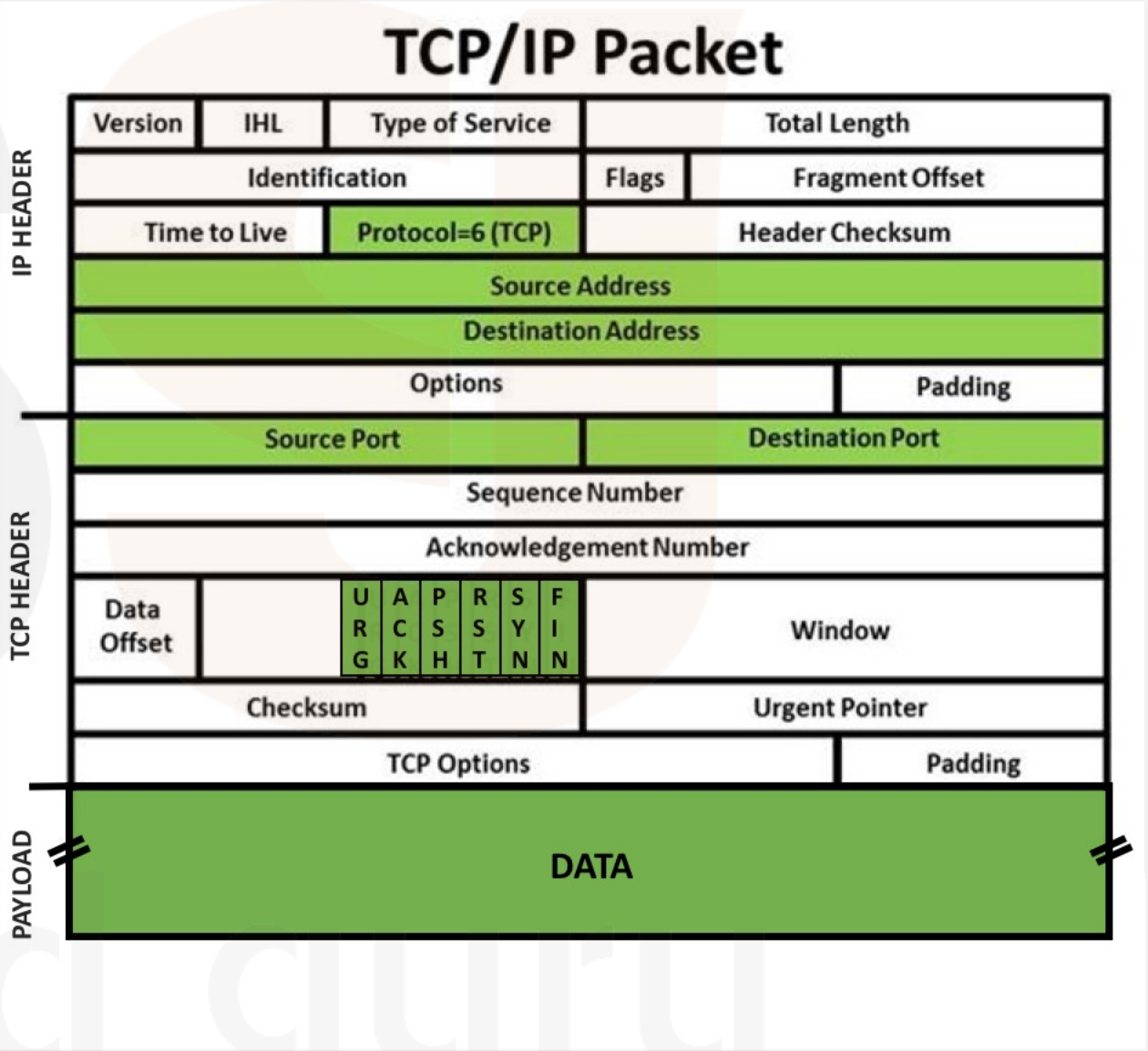
Explain Packet Structure.

A packet has 3 main sections

- IP Header
- TCP Header
- Payload

Few of the important fields in the packets are

- Source IP
- Destination IP
- Source Port
- Destination Port
- TCP Flags
- Data



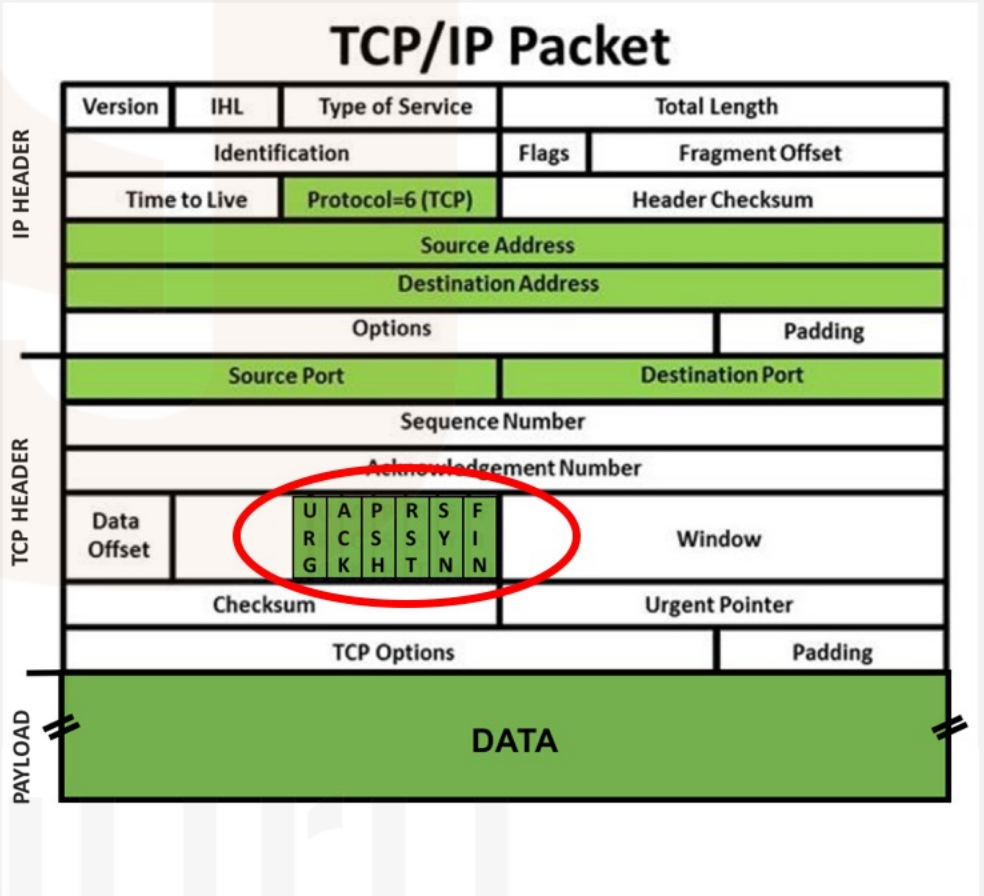
anand guru

Explain TCP Flags.

In TCP connection, flags are used to indicate a particular state of connection.

There are 6 Flags in a TCP Header

Flag	Description
SYN (Synchronization)	It is used in first step of connection establishment phase or 3-way handshake process between the two hosts.
ACK (Acknowledgement)	It is used to acknowledge packets which are successful received by the host.
FIN (Finish)	It is used to request for connection termination i.e. when there is no more data from the sender, it requests for connection termination.
RST (Reset)	It is used to terminate the connection if the RST sender feels something is wrong with the TCP connection or that the conversation should not exist
PSH (Push)	It tells the receiver to process these packets as they are received instead of buffering them.
URG (Urgent)	Data inside a segment with URG = 1 flag is forwarded to application layer immediately even if there are more data to be given to application layer.



Explain OSI Reference Model.

Layer No.	Layer	Function	Devices	Protocols	PDU (Protocol Data Unit)
7	**APPLICATION**	• Interface between User and Computer. It provides services to the user. • Applications produce the data, which has to be transferred over the network.	-	HTTP, SMTP	Data

6	**PRESENTATION**	• The data from the application layer is extracted here and manipulated as per the required format to transmit over the network.
		  • Translation (ASCII to HEX) • Encoding/Decoding
		  • Encryption/Decryption • Compression
			-	JPEG, MPEG, TLS, SSL	Data

5	**SESSION**	• This layer is responsible for establishment of connection, maintenance of sessions, authentication and also ensures security.	-	NetBIOS, NFS, RPC	Data
4	**TRANSPORT**	• It provides reliable message delivery from process to process • Ensures that messages are transmitted in the order in which they are sent and there is no duplication of data. • It is also responsible for error control and flow control	-	TCP/UDP	Segments
3	**NETWORK**	• Network layer works for the transmission of data from one host to the other located in different networks. • Takes care of packet routing i.e. selection of the shortest path to transmit the packet, from the number of routes available.	Routers, Firewall, IPS	RIP, OSPF	Packets

2	**DATA LINK**	• The data link layer is responsible for the node to node delivery of the message.
		• It does Framing, error control, flow control etc.
		• Data Link Layer is divided into two sub layers :
		  • Logical Link Control (LLC)
		  • Media Access Control (MAC)
			Switch	ARP	Frames

1	**PHYSICAL**	• It is responsible for the actual physical connection between the devices.	Hub, Bluetooth, WiFi	802.11	Bits

Explain OSI model with an example.

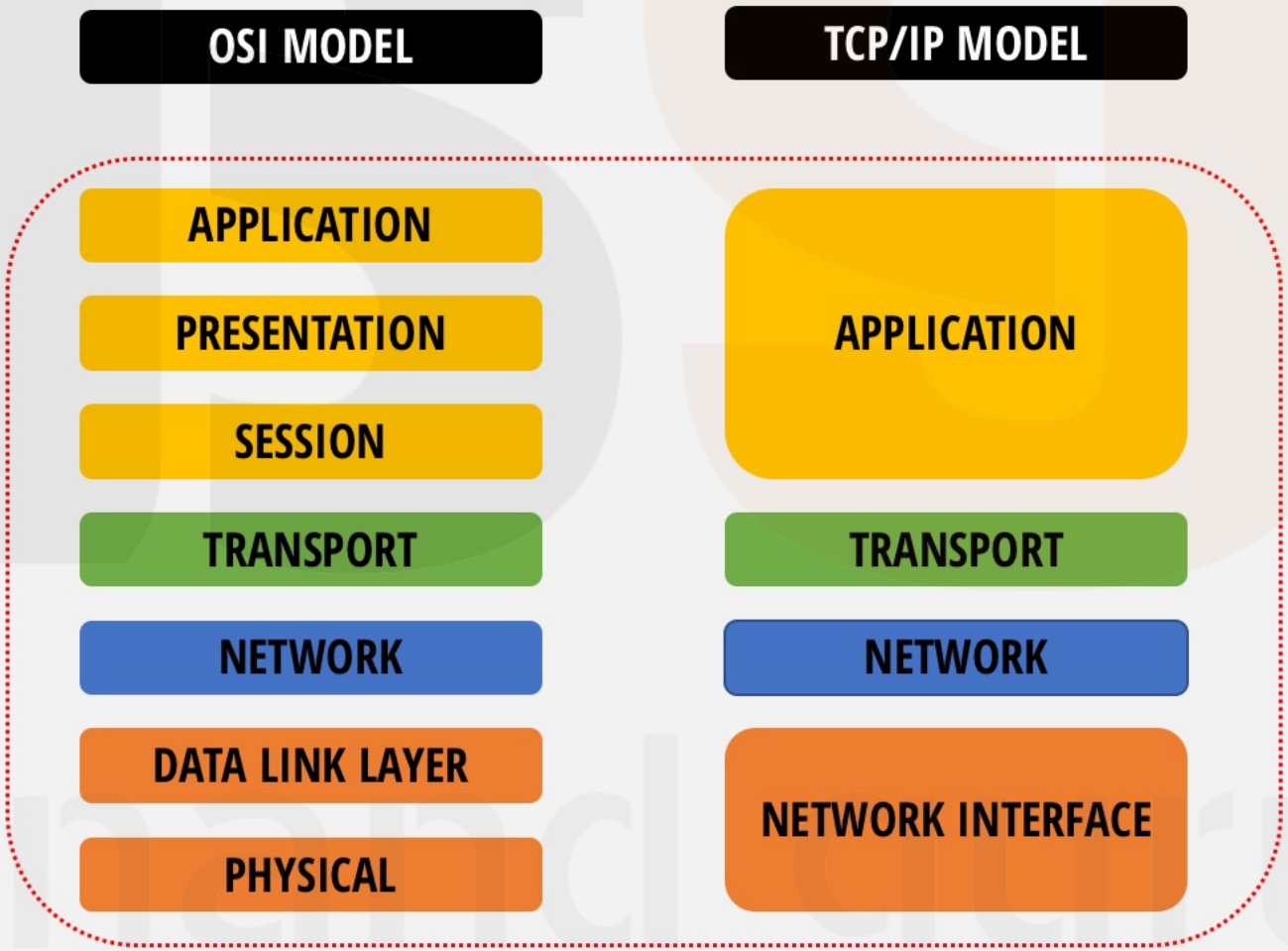
Lets discuss how email flows between sender and recipient using OSI model.

1. Sender uses an application like Outlook to compose and send the email. - **APPLICATION**
2. The email is encoded, encrypted (if enabled) and compressed. - **PRESENTATION**
3. The sending server initiates the connection with the receiving server. - **SESSION**
4. The entire email flows is done error free, receiving acknowledges. - **TRANSPORT**
5. Each packet will be routed from sender email server to recipient email server. - **NETWORK**
6. Node to Node transmission happens using next hop's MAC address. - **DATA LINK LAYER**
7. All the data is transmitted as bits through cables or wireless signals. - **PHYSICAL**

One the recipients side, the data moves from cable to users machine, where the presentation layer will take care of decoding, decrypting and decompressing the data. Finally the Outlook application will display the message to the recipient

Explain TCP/IP Model

OSI is a reference model, where as TCP/IP model is a practical model. The functions remain the same, but few of the layers gets merged in TCP/IP model.



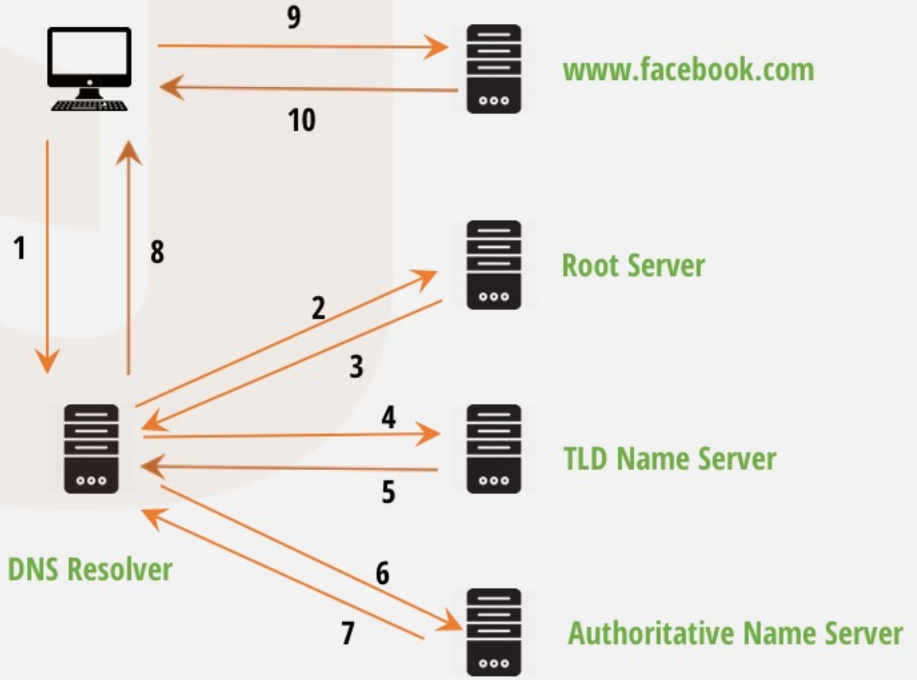
What is DNS and how it works?

DNS stands for Domain Name System.

It is a service that helps in translating domain names to IP addresses and vice versa.

How DNS works?

- When a computer needs to reach to a domain (like facebook.com) it sends a request to a server called **DNS Resolver** (DNS server). If the mapping is found for the domain in the DNS cache, the server returns the IP address. If not,
- The Resolver reaches out to **Root Server**. Root Servers hold the index of a Top Level Domains. There are 13 root servers globally.
- **TLD Name Server** gives the IP address of the Authoritative Name Server that holds the mapping for the requested domain name.
- If the **Authoritative Name Server** has access to the requested record, it will return the IP address
- This address is return to the client that made the original request.
- The client now makes the request to the IP address and get the response



DNS follow-up questions.

Does DNS use UDP or TCP?

DNS uses both TCP and UDP

UDP for DNS Queries

TCP for Zone Transfers

DNS Records Types.

A	(Host address)
AAAA	(IPv6 host address)
ALIAS	(Auto resolved alias)
CNAME	(Canonical name for an alias)
MX	(Mail eXchange)
NS	(Name Server)
PTR	(Pointer)
SOA	(Start Of Authority)
SRV	(location of service)
TXT	(Descriptive text)

anand guru

What is DHCP and how it works?

DHCP stands for Dynamic Host Configuration Protocol.

DHCP server automatically assigns an IP address and other information to each host on the network so they can communicate with other endpoints.

How DHCP works?

DHCP works on a process called DORA.

- When a computer that is configured to get the IP details automatically is powered on, it sends DHCP **DISCOVER** message to all hosts.
- After the DHCP Server receives discover message it suggests the IP addressing offering to the client host by unicast.
  This **OFFER** message contains: IP Address, Subnet mask, Default Gateway, DNS and Lease period
- Now after the client receives the offer it requests the information officially sending **REQUEST** message to server this time by unicast.
- Server sends **ACKNOWLEDGE** message confirming the DHCP lease to client. Now client is allowed to use new IP settings.

DHCP follow-up questions.

What will the IP address of the client machine when it sends DISCOVER message?

The Source IP will be 0.0.0.0

How does client knows the IP address of the DHCP Server, to send a Discover message?

The client would not be knowing the DHCP address, hence it broadcasts the Discover message. i.e. Destination IP will be 255.255.255.255

What happens if no DHCP server is available on the network?

The client gets an IP is the APIPA (Automatic Private IP Addressing) range. The range is between 169.254.0.0 - 169.254.255.255

What happens when the DHCP server runs out of IP addresses?

When you start running out of addresses, your subnet is said to be oversubscribed. Then the DHCP server refuse to assign an IP address until a device in the network releases an IP address and makes it available again or the lease time expires.

Explain ARP.

ARP stands for Address Resolution Protocol.

It helps to resolve an IP address to physical address (MAC Address)

How ARP works?

1. When a source device want to communicate with another device, source device checks its Address Resolution Protocol (ARP) cache to find it already has a resolved MAC Address of the destination device. If it is there, it will use that MAC Address for communication. If not, the source broadcasts the Address Resolution Protocol (ARP) request message to the local network.
2. The message is received by each device on the LAN since it is a broadcast. When the destination device receives the ARP request, it will send the Address Resolution Protocol (ARP) reply message to the source as a unicast.
3. The source machine will update its Address Resolution Protocol (ARP) cache.

anand guru

What are proxy servers and how do they protect computer networks?

Proxy servers processes the request on behalf of other machines. The IP address is converted by NAT process.

Proxy servers primarily prevent external users from identifying the IP addresses of an internal network.

Without knowledge of the correct IP address, even the physical location of the network cannot be identified.

Proxy servers can make a network virtually invisible to external users.

anand guru

When you use a proxy, is DNS query done by client or Proxy server?

It depends on the type of proxy being used.

If it is a simple **IP proxy**, then the client will do a DNS query, resolve the destination domain name and send the request to proxy.

If the proxy is a **HTTP proxy (Web Proxy),** the client directly send the request to proxy. Proxy requests for DNS resolution and forward the traffic.

anand guru

Few random questions

Can you connect 2 computer directly?

Yes, with the help of cross-over cables.

I give you a new laptop, explain how you will connect to internet.

- Assuming the OS is already installed. I will look to assign the IP details like
  - IP Address
  - Subnet Mask
  - Default Gateway
  - DNS Server
- I will get these details from the network engineer who has designed the network.
- Alternately, if I there is a DHCP server in the network, I will configure the new laptop to automatically get the IP details.
- Then I ping any public IP like 8.8.8.8 to confirm if the laptop is able to reach the internet
- Also, ping any URL like www.google.com to check if DNS is working fine.

ICMP works on which layer?

ICMP works on Layer 3.

What port does ping use?

Ping uses ICMP(Internet Control Message Protocol). it does not use TCP or UDP. To be more precise ICMP type 8 (echo request message) and type 0 (echo reply message) are used. ICMP has no ports.

What happens when you type-in an URL (like www.goolgle.com) in your browser and press enter?

When you type in www.google.com into the address bar of browser,

1. The client needs to finds the IP address of the URL (in this case google.com).
    1. Browser check for if its cache to see if it has the IP address for entered domain
    2. If there is no IP mapping, it will check in OS cache.
    3. If the OS cache also doesn't have the IP address, the client initiates a DNS request to the configured DNS server.
2. Once the client has the IP address of the URL, the browser initiates a TCP connection with the server.
3. The browser sends an HTTP request to the webserver.
4. The server handles the request and sends back a response.
5. The browser displays the HTML content

anand guru

Firewall related questions.

What is Firewall?

A firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules (ACL – Access Control List). Traditional firewalls works at Layer 3 and Layer 4.

When we can write ACLs in Router, why we need a Firewall?

Primary function of a router is to route the traffic. If we add packet filtering functions on to the router, it will slow down the network.

Hence it is a good practice to separate filtering and routing functionality

What is DMZ?

DMZ stands for DeMilitarized Zone. It is a network segment used to host public facing servers. The DMZ isolates the public facing servers from internal servers. So if the servers in DMZ are compromised, the attack doesn't spread to internal network.

What is Implicit Deny?

If traffic is not explicitly allowed within an access list then by default it is denied

What is the difference between Firewall Deny and Drop?

When the firewall is set to Deny a connection, it blocks the connection and sends a Reset (RST) packet to the requester (source).

When the firewall is set to Drop a connection, it just drops the requests without giving any message to the requester.

It is good practice to Deny outbound traffic and Drop inbound traffic, so the attacker will not know the presence of the Firewall.

What is Stateful Inspection?

A stateful firewall maintains a table of active connections it has allowed in a State Table. Further packets associated with the session are permitted to pass through the firewall.

What is VPN?

A virtual private network (VPN) extends a private network across a public network, and enables users to send and receive data across public networks as if they were directly connected to the private network.

There are 2 types of VPN: **Site-to-Site VPN** – Used to connect two office locations. **Remote VPN** – Used by users to connect to corporate network

IPS/IDS related questions.

What is IDS?

An Intrusion Detection System is a network security solution that detects the malicious traffic based on the signatures. IDS systems compare the current network activity to a known threat database (network signatures) to detect several kinds of behaviors like security policy violations, malware, and port scanners.

Difference between IPS and IDS.

IDS scans the traffic and detects malicious traffic and report it to the admin based on network signature.

IPS scans the traffic, detects and can also block (prevent) the malicious traffic based on network signatures.

Explain IDS Signature syntax.

```
alert icmp any any -> $HOME_NET any (msg:"ICMP test"; sid:1000001; rev:1; classtype:icmp-event;)
```

Rule Header

`alert` – Rule action. Snort will generate an alert when the set condition is met.
`any` – Source IP. Snort will look at all sources.
`any` – Source port. Snort will look at all ports.
`->` – Direction. From source to destination.
`$HOME_NET` – Destination IP. We are using the HOME_NET value from the snort.conf file.
`any` – Destination port. Snort will look at all ports on the protected network.

Rule Options

`msg:"ICMP test"` – Snort will include this message with the alert.
`sid:1000001` – Snort rule ID.
`rev:1` – Revision number. This option allows for easier rule maintenance.
`classtype:icmp-event` – Categorizes the rule as an "icmp-event", one of the predefined Snort categories.

Difference between IPS and Firewall.

A firewall inspects TCP/IP header working on ACLs.

IPS does deep packet inspection (checks both header and payload) using network signatures

Where do you place IPS?

An IPS is usually placed after the Firewall. Firewall does the heavy lifting of blocking all the unwanted traffic based on TCP/IP header. And of the traffic that is allowed, IPS will do deep packet inspection. Because of this IPS needs more processing power than a firewall.

If IPS is placed first, it will unnecessarily do deep packet inspection on all the traffic, while a good amount of traffic could have been blocked just by inspecting TCP/IP header with a packet filtering device like Firewall.

Questions on Linux commands

Sl. No.	Question	Command
1	Change Directory	**cd**
2	How do you check running process?	**ps auxf**
3	Disk statistics.	**df -h**
4	How do you find a file on Linux?	**find / <name_of_file>**
5	How do you kill a process in Linux?	**kill -9 <process_id>**
6	How do you get help on a command?	**man top** **top --help**
7	Create a new directory	**mkdir <new_directory_name>**
8	Change password	**passwd**
9	Present working directory	**pwd**
10	How do you open a text file to see the latest (last lines) during troubleshooting?	**tail –f <file_name>**
11	How do you display data regarding RAM and CPU?	**top**
12	Packet capture	**tcpdump –vvnni eth0**
13	How do you find the IP address on a Linux machine?	**ifconfig**